

Web Images Videos Maps News Shopping Gmail more ▾

Web History | Search settings | Sign in



fast, AES, Rijndael, block cipher

Search

Advanced Search

Web Show options...

Results 1 - 10 of about 72,600 for fast, /

### Advanced Encryption Standard - Wikipedia, the free encyclopedia

Jump to Description of the **cipher**: Unlike most other **block ciphers**, **AES** has a very neat algebraic description. .... Improved Cryptanalysis of **Rijndael**, **Fast** Software Encryption, ...  
en.wikipedia.org/wiki/Advanced\_Encryption\_Standard - Cached - Similar

### New Attacks on AES / Rijndael

**Fast** Algebraic Attacks on **Block Ciphers** and Courtois Toy Cipher. .... The Security of **Rijndael/AES** and the XSL Attack on **Block Ciphers**. ...  
www.cryptosystem.net/aes/ - Cached - Similar

### Nicolas T. COURTOIS' research in cryptography

Nicolas T. Courtois: How **Fast** can be Algebraic Attacks on **Block Ciphers**?, .... my **AES / Rijndael** page with the latest news about algebraic attacks on **AES**. ...  
www.cryptosystem.net/~courtois/myresearch.html - Cached - Similar

### AES - Rijndael

The Advanced Encryption Standard (**AES-Rijndael**) cores for ASICs and FPGAs are .... Hardware cores for the following other symmetric-key **block ciphers** have been ... K. Gaj and P. Chodowiec, "**Fast** implementation and fair comparison of the ...  
ece.gmu.edu/crypto/rijndael.htm - Cached - Similar

### A methodology to implement block ciphers in reconfigurable ...

A methodology to implement **block ciphers** in reconfigurable hardware and its application to **fast** and compact **AES RIJNDAEL**. Full text, Pdf (237 KB) ...  
portal.acm.org/citation.cfm?id=611849 - Similar  
by FX Standaert - 2003 - Cited by 40 - Related articles

### [PDF] AES Finalist Algorithm: The Rijndael Block Cipher

File Format: PDF/Adobe Acrobat - Quick View

**AES** Finalist Algorithm: The **Rijndael Block Cipher**. Mel Tsai .... An entire round can be implemented via a **fast** table lookup routine on ...  
www.mtsai.net/documents/rijndael\_presentation.pdf - Similar

### IAIK - TU Graz :: AES Lounge

**Rijndael**. **AES** Security. **AES** Hardware Architectures .... **Fast** implementations of secret-key **block ciphers** using mixed inner- and outer-round pipelining ...  
www.iaik.tugraz.at/content/research/krypto/AES/ - Cached - Similar

### AES IP Core - AES-C Advanced Encryption Standard FIPS-197 Secure ...

The **Fast** version can achieve throughput rates of 2 Gbps or more in FPGAs, ... Block Diagram. **AES (Rijndael)** Encrypt/Decrypt IP core block diagram (**AES-C**) ... It operates in any one of the common **block cipher** modes (ECB, CBC, CFB, OFB, ...  
www.cast-inc.com/cores/aes-c/index.shtml - Cached - Similar

### CommsDesign - Digital Cryptography: Rijndael Encryption and AES ...

The **Rijndael** algorithm is a symmetric iterated **block cipher**. ... Very **Fast AES** products target applications with data rates faster than 2000 Mb/s/sec. ...  
www.commsdesign.com/showArticle.jhtml?articleID... - Cached - Similar

### Free aes rijndael cipher Download

It is **fast**, easy-to-use ... Amethyst CIPHER is the single-click s. dgEncrypt 2.0. dgEncrypt is

an implementation of the **Rijndael block cipher**, ...  
wareseeker.com › Free Download Search - [Cached](#)

Searches related to: **fast, AES, Rijndael, block cipher**

- |  |   |  |                                      |
|--|---|--|--------------------------------------|
| <a href="#">twofish block cipher</a>   | <a href="#">rijndael block cipher algorithm</a> | <a href="#">block ciphers stream ciphers</a> | <a href="#">serpent block cipher</a> |
| <a href="#">symmetric block cipher</a> | <a href="#">rsa block cipher</a>                | <a href="#">rc6 block cipher</a>             | <a href="#">des block cipher</a>     |

1 2 3 4 5 6 7 8 9 10    **Next**

Search

[Search within results](#) - [Language Tools](#) - [Search Help](#) - [Dissatisfied? Help us improve](#) - [Try Google](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [Privacy](#) - [About Google](#)

Web Images Videos Maps News Shopping Gmail more ▾

Web History | Search settings | Sign in





[Advanced Search](#)

Web [Show options...](#)

Results 1 - 10 of about 22,700 for compact, /

### A methodology to implement **block ciphers** in reconfigurable ...

A methodology to implement **block ciphers** in reconfigurable hardware and its application to fast and **compact AES RIJNDAEL**. Full text, Pdf (237 KB) ...

[portal.acm.org/citation.cfm?id=611849](http://portal.acm.org/citation.cfm?id=611849) - [Similar](#)

by FX Standaert - 2003 - Cited by 40 - [Related articles](#)

### [PDF] The Rijndael Block Cipher

File Format: PDF/Adobe Acrobat - [Quick View](#)

-RDQ 'DHPHQ. 9LQFHQW 5LMPHQ. The **Rijndael Block Cipher**. AES Proposal ....

**Compact** co-processor on a Smart Card to speed up **Rijndael** execution: for this ...

[www.daimi.au.dk/~ivan/rijndael.pdf](http://www.daimi.au.dk/~ivan/rijndael.pdf) - [Similar](#)

by J Daemen - Cited by 834 - [Related articles](#) - All 192 versions

### An FPGA implementation of the **AES-Rijndael** in OCB/ECB modes of ...

OCB assumes a fixed length **block cipher** (such as **AES**). .... size for the key as being commonly usable while being more **compact** than other implementations. ...

[linkinghub.elsevier.com/retrieve/pii/S0026269204001636](http://linkinghub.elsevier.com/retrieve/pii/S0026269204001636) - [Similar](#)

by C Chiju - 2005 - Cited by 6 - [Related articles](#)

### **AES** IP Core - **AES-C** Advanced Encryption Standard FIPS-197 Secure ...

The Standard version is more **compact**, using a 32-bit datapath and requiring four clock ...

**AES (Rijndael)** Encrypt/Decrypt IP core block diagram (**AES-C**) ... It operates in any one of the common **block cipher** modes (ECB, CBC, CFB, OFB, ...

[www.cast-inc.com/cores/aes-c/index.shtml](http://www.cast-inc.com/cores/aes-c/index.shtml) - [Cached](#) - [Similar](#)

### CommsDesign - Digital Cryptography: **Rijndael** Encryption and **AES** ...

The **Rijndael** algorithm is a symmetric iterated **block cipher**. ... The **Compact AES** products are perfect solutions for wireless applications, such as PDAs and ...

[www.commsdesign.com/showArticle.jhtml?articleID...](http://www.commsdesign.com/showArticle.jhtml?articleID...) - [Cached](#) - [Similar](#)

### Ultra-Compact AES IP Core

Ultra-**Compact** Advanced Encryption Standard (**AES**) Core ... Encrypts using the **AES Rijndael Block Cipher** Algorithm. Satisfies Federal Information Processing ...

[www.ipcores.com/Ultracompact\\_AESCore.htm](http://www.ipcores.com/Ultracompact_AESCore.htm) - [Cached](#) - [Similar](#)

### New Attacks on **AES** / **Rijndael**

The Security of **Rijndael/AES** and the XSL Attack on **Block Ciphers**. Nicolas Courtois and Josef Pieprzyk: ... (Contains the so called "**compact** XSL attack"). ...

[www.cryptosystem.net/aes/](http://www.cryptosystem.net/aes/) - [Cached](#) - [Similar](#)

### A **Compact** Piplined Hardware Implementation of the **AES-128 Cipher**

Implement **Block Ciphers** in Reconfigurable Hardware and its Application to Fast and **Compact AES RIJNDAEL**, in Proceedings of FPGA, 2003. ...

[doi.ieeecomputersociety.org/10.1109/ITNG.2006.1](http://doi.ieeecomputersociety.org/10.1109/ITNG.2006.1) - [Similar](#)

by N Nedjah - All 4 versions

### [PDF] Efficient Implementation of **Rijndael** Encryption in Reconfigurable ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

A.Satoh et al, **Compact** Hardware Architecture for 128-bit **Block Cipher** Camellia, in the ... Hardware and its Application to Fast and **Compact AES Rijndael**, in ...

[www.intopix.com/pdf/2\\_efficient\\_implementation\\_of\\_rijndael.pdf?...](http://www.intopix.com/pdf/2_efficient_implementation_of_rijndael.pdf?...)

by FX Standaert - Cited by 83 - Related articles - All 9 versions

LNCS 2851 - Hardware-Focused Performance Comparison for the ...  
more than 20 years, and is a subset of the SPN cipher **Rijndael** [5] ..... **Compact** and high-  
speed architectures for the 128-bit **block ciphers AES** and Camel- ...  
[www.springerlink.com/index/42GLQK35TNJAY94K.pdf](http://www.springerlink.com/index/42GLQK35TNJAY94K.pdf) - Similar  
by A Satoh - Cited by 8 - Related articles - All 5 versions

Searches related to: **compact, AES, Rijndael, block cipher**

[block cipher encryption](#)

[block ciphers stream ciphers](#)

[rijndael block cipher algorithm](#)

[rsa block cipher](#)

1 2 3 4 5 6 7 8 9 10

[Next](#)

---

[Search within results](#) - [Language Tools](#) - [Search Help](#) - [Dissatisfied? Help us improve](#) - [Try Google](#)

---

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [Privacy](#) - [About Google](#)